Fraud Risk Assessment Plan for Barclays Bank of Kenya

Janet Kimani

Bachelor's thesis
December 2011
Degree Programme in International Business
Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

Tampere University of Applied Sciences

Degree Programme in International Business

Author: Janet Kimani

Title: Fraud Risk Assessment Plan for Barclays Bank of Kenya

Number of pages: 66 (65 + appendix)

Graduation Time: December 2011

Thesis Supervisor: Pasi Kuusijärvi

Commissioned by: Barclays Bank of Kenya

ABSTRACT

The typical organization loses an average of 5-7% of its gross revenue to fraud annually. Theft of assets, which includes money, physical assets and or services, is the most common type of fraud. Majority of frauds are detected through tips reported by either employees, vendors or whistle blowers. Organizations that implement company-wide fraud awareness training cut fraud losses by 52%.

This thesis aims at providing more understanding of fraud; prevention, detection, reporting and resolution guidelines which the Bank can incorporate in its fight against fraud.

The commissioner of this thesis, Barclays Bank of Kenya, is one of the leading banks in the country and has operated in Kenya for almost 100 years. The Bank is highly respected for its outstanding performance over the years and its overall image. Unfortunately, like many other organizations, the Bank continues to face fraud committed by its employees and or third parties.

Fraud risk assessment provides a comprehensive step by step model that can be utilized in identifying the methods through which fraud is committed, preventing further fraudulent activities occurring and providing guidelines of handling fraud and taking action against perpetrators. Fortunately, some fraud risks are preventable, while others can be closely monitored in order to reduce their consequences and frequencies of occurrence.

Reducing fraud to the minimum will help Barclays Bank to streamline its business through improving the quality of its processes and ultimately the quality of services offered to customers. This will in turn build customer confidence and increase the Bank's reputation in comparison to its competitors.

This thesis contains some confidential information that does not appear on the published version.

Key words: Barclays Bank of Kenya, fraud, total quality management, risk Management

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

‘A way of making money is to stop losing it.’

Despite the size and area of business that organizations operate in, they are constantly exposed to operational risk. Operational risk is the loss resulting from inadequate or failed internal processes, people and systems, or from external events. It is also the widest category of risk, bounded only by subjects such as Murphy’s Law which states that “anything that can go wrong will go wrong”, the imagination of fraudsters, and external events completely beyond management’s control. Operational risk is therefore the first type of risk that any institution takes on. Managing and mitigating the operational risk of an organization is a significant challenge for senior managers. (Adam 2005, 130).

A vast amount of resources, time and energy are used up in developing Corporate Governance Policies, implementing internal control systems, risk management strategies and training employees to adhere to these measures. Yet, some dishonest, intelligent people, commonly referred to as fraudsters, still manage to find ways to override systems or dupe honest people in to gaining access to organizations’ resources and assets.

The unfortunate truth is that a majority of organizations that fall victim to fraud do not take the time to fully understand the actual risks involved in fraud and therefore do not make efforts to detect and prevent fraud before it actually occurs. Rather than taking preventative measures against fraud, many executives tend to rely on the belief that people are honest and cannot commit fraud.

Research shows that there is not a single financial organization that is immune to fraud, and that the typical organization loses 5-7% of its annual revenues to fraud. (Samociuk, Iyer & Doody 2010, 11).

Developing preventative measures against fraud, identifying the methods through which fraud is or can be committed, establishing effective control measures and putting in

place fraud resolution guidelines not only helps organizations prevent the loss of revenue and assets, but also improves the quality of their business processes and their overall reputation in the business environment.

GOAL AND METHODOLOGY

The final outcome of this thesis is to create more understanding of fraud in Barclays Bank of Kenya; finding ways of detecting fraud before it actually occurs, improving the existing fraud detection systems, reporting guidelines for fraud, managing fraud and resolution guidelines of dealing with fraud.

By so doing, this information will be useful in reducing fraud committed within and against the Bank to the minimum and improve the quality of business processes carried out by the bank, its ethical organizational culture and the quality of output provided by employees of the bank.

Improving the quality of processes and output in the Bank will ultimately provide a competitive strategy for the Bank. Total Quality Management principles insist that business strategy must be firmly based on an effective customer strategy.

The findings of this thesis will not only be beneficial to the Barclays Bank of Kenya, but also to other banks and organizations operating in Kenya. Fraud is quickly becoming a rising industry in Kenya and if nothing is done to fight it now, some existing businesses will collapse, foreign investors will be discouraged to make investments in the country and crime rate will reach its peak.

2.1 Qualitative and Quantitative Research

Qualitative research aims at gathering an in-depth understanding of the ‘why’ and ‘how’ of decision making. Since qualitative research usually involves a small but focused sample group, data collected can vary considerably. This is the reason why the role of the researcher in qualitative research is vital. Data collected through qualitative research

cannot always be put into a context that can be graphed or displayed as a mathematical term.

Quantitative research on the other hand seeks to measure and analyse data in a mathematical manner. The subject at hand in quantitative research is usually familiar. The target research group can be quite large, depending on the research topic and purpose of the study. Research questions are usually standardized and are used to test assumptions. The information gathered from the target sample in quantitative research is used to draw conclusions about the rest of the general population. (Glenn 2010, 105).

This thesis is primarily a case study, which is a form of qualitative research. This case study seeks to understand fraud in Barclays Bank of Kenya; the methods through which fraud is committed by both internal and external fraudsters, evaluate the control measures in place, the fraud response actions taken by the Bank and finally how resilient the bank is to fraud.

With this information, recommendations will be made on how best to reduce fraud through preventative measures, detection of fraud before it actually occurs, resolution guidelines and risk management.

2.2 Data collection

Data collection refers to the sources and methods used to gather data to be analyzed, from which conclusions are drawn and recommendations put forward.

This thesis is a case study which is a form of qualitative research. Several methods will be used to collect data. Primary sources of data include interviews in form of a questionnaire which will be directed to the fraud specialists in the Bank.

Majority of the data collected, however, will be from secondary sources. Secondary sources of information are those that have been collected and compiled by other people, other than the writer herself. These sources of information include publications such as journals, books, organizational publications and internet sources such as web pages.

3 THEORETICAL FRAMEWORK

3.1 Total Quality Management (TQM)

The circle of quality begins and ends with the customer. Customer requirements for products and services established through market research and feedback systems are integrated in the product design. During the product development process, organizations aim at adding value and improving the quality of products and processes. Total Quality Management focuses on improving quality throughout the organization with emphasis on the customer; as opposed to traditional quality management which focused on improving the quality of final goods.

In the face of diminishing resources and the current political & economic environment, the demand for quality in all of an organization's business practices is absolute. Increased competition means not just fair prices but also provision of high quality goods and services. Customers are becoming increasingly intolerant of poor quality goods and services and are exerting control over organizations by opting to buy from alternative sources. Improving the quality of products and services to obtain an edge over competitors will in the long run elevate organizations to become more reputable.

3.1.1 Levels of quality management in Barclays Bank of Kenya

The organisational level

This level seeks to meet external customer requirements therefore requiring regular customer input. Market researches, research and development and customer complaints are sources of information regarding customer requirements for goods and services.

Barclays Bank of Kenya could use customer-driven performance standards as the basis for goal setting in order to motivate its employees to perform. Such standards include performance appraisals, incentive compensation, non-financial rewards and resource allocation. This is the level where top management of the bank should focus most of its

attention to ensure that the goal towards quality improvement is understood and utilized in order to meet and exceed customer requirements.

The process level

Organizations are divided into different functions such as marketing, design, product development, operations, and so on. Processes carried out in these departments are cross-functional therefore if managers of different departments of the Bank optimise the processes and activities under their control, they consequently sub-optimize activities for the Bank as a whole.

The performer/ job level

The Bank's employees play a vital role in delivering goods and services to its customers. Output standards must be based on quality and customer-service requirements which arise from the Bank's organizational and process levels. These standards include requirements for accuracy, completeness, innovation, timeliness and cost. This level calls for all Bank employees to understand the roles and responsibilities in their jobs in the ultimate pursuit of quality.

3.1.2 Quality as a source of value for Barclays Bank

Improving quality can prove beneficial in many ways to organizations. Bhat (2010, 23-24) summarizes the main benefits as:

Quality and profitability

According to Jeyarathmm (2008, 88) quality influences greater efficiency, higher productivity and high quality goods and services. This means that less time is spent reworking and correcting mistakes that were committed earlier due to carelessness or negligence.

High quality products and services create strong brands and reputation, which in turn permits the company to charge higher prices for their products. (Jeyarathmm 2008, 88).

As shown in figure 1, high quality will increase the Bank's ability to compete in the market place and reduce production costs. Improving quality in the Bank can increase its market share and reduce the cost of producing services which in turn will increase profits.

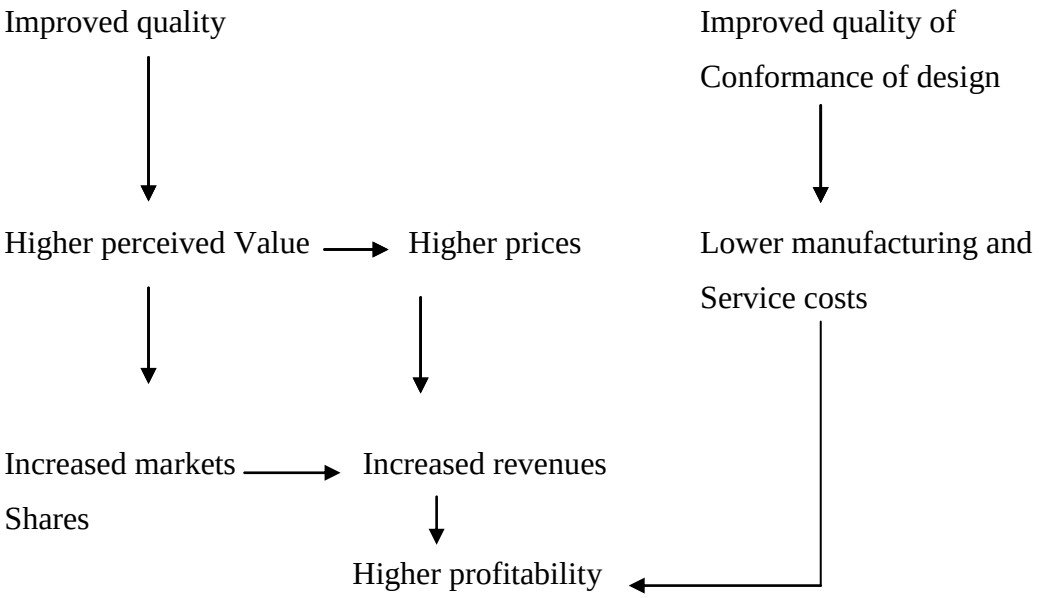

FIGURE 1. Impact of Quality on Profits

Source: James R. Evan and William M. Lindsay, "The Management and Control of Quality", 4th Edition, South-Western College Publishing, p. 22.

The challenge for any business today is to produce quality products or services efficiently. Profitability comprises productivity, operation costs and the quality of the goods and services produced. Of these three determinants of profitability, the most significant in determining the long-run success or failure of any organisation is quality. (Bhat 2010, 6).

Improved reputation

Quality has been recognized as having a significant impact on the development and maintenance of a sustainable competitive advantage. A majority of customers regard quality as an important source of value.

Good quality not only increases the Bank's profitability and productivity but also improves its brand image and ultimately its overall image. Most importantly, customers who are satisfied with the quality of goods and service provided by the Bank will usually reward the Bank with continued patronage and favourable word-of-mouth advertising.

Reduced costs & Improved Productivity

In the short-term, creating competition based on quality creates paradox for a company. This is because improving quality requires a lot of resources and money which directly increases the operating costs of a company.

However, in the long term, eliminating quality related problems in Barclays will help reduce costs because it eliminates constant inspections and recalls. Improved quality will result in reduced wastages and reduced costs (due to elimination of inspection and rework) and thereby improving productivity.

Easier Selling

Barclays Bank's brand is what differentiates its products or services from its competitors. Brand recognition creates a sense of identity, or what their brands stand for. While it's certainly true that lesser known organizations must work hard at cultivating their brand image, even household giant names have to work at brand redevelopment. The bottom line is every organization needs to hone its brand image. (Arthur 2005, 11).

Employer Pride

Most employees, both regular workers and managers are generally proud to be associated with a company that has a strong public image and is a provider of high quality products and services. Employees are motivated by knowledge that they produce some of the best products and services in the industry.

Unfortunately, despite widespread awareness of the importance of quality, many companies still struggle to integrate quality into their management efforts. The shift towards

quality has resulted in many successes, but also in many failures. Usually when an initiative toward emphasis on quality fails, it is generally because of poor management, not the soundness of principles.

3.1.3 Relationship between quality and different company functions

Inspection alone cannot build quality into a product unless quality has been designed and manufactured into it. Quality awareness must begin at the very conception of the product and continue throughout the various stages of its development. During its usage, the product should also meet the required quality standards. This helps to provide feedback which is so essential for quality improvement. (Lal 2008, 25).

When carrying out market research, quality engineers assist customers to decide what is required of products. Sometimes, however, carrying out prior market researches cannot be conducted to avoid leaking information about new products to competitors. In such instances, product designers, quality engineers and marketers have to assume the role of the customer and decide about the desirable features in the proposed product. (Lal 2008, 31).

According to Bhat (2010, 38) the relationship between quality and various departments in an organization can be summed up as:

Marketing and Sales: Personnel in these departments collect vital information regarding customer preferences and feedback on existing products. They are also responsible in providing technical advice on how to use the products and services. This information is then used to develop products and services that provide utmost satisfaction to customers.

Research & Development (R&D): All industries need to establish ways to predict the future in terms of products, sales, business environment and competition. Industries that operate in fast changing environments must continually revise their design and range of products. This is the only way to ensure the survival of a company. Without R&D, firms are forced to rely on strategic alliances, acquisitions, and networks to tap into the innovations of others.

This function of an organization is therefore responsible in keeping track of the changing needs and preferences of customers, studying competitor strategies and reviewing the design prototypes in accordance to customer preferences.

Design and Engineering: These departments are responsible for developing the technical specifications of products and services. They formulate inspection procedures, investigate defects and come up with processes to improve the quality of goods.

Purchasing and Receiving: They are responsible for preparation of procurement specifications for materials and bought out components and evaluating suppliers. The quality of raw materials directly affects the quality of end products; only suppliers with high quality materials and parts should be selected to avoid compromising the quality of goods.

Quality Control: This staff function is concerned with the prevention of defects in manufacturing so that the items may be manufactured right at the first time and not have to be reworked or rejected. In order to achieve this, there must be inspection and control of incoming raw materials to ensure that they meet the specifications, in-process inspection of manufacturing processes and final inspection and testing of the finished product to be delivered to the customers.

A quality control system is designed to ensure economical production of products of uniform quality which is acceptable to the customer. The modern approach of quality control calls for preventative measures against defective goods and services provided. It requires establishment of quality control systems which are designed to prevent defects from occurring and should be aimed at continuous improvement of quality. (Bhat 2010, 41-43).

Production: This department is responsible for the production of goods. Production involves process planning and conducting process capability studies. They also formulate inspection procedures, investigate defects and their causes, analyze the quality of products and oversee the operation controls.

In the service industry, this function falls directly on customer service employees. In order for companies to provide services to their customers, there has to be two key important elements; the employees (human resources) who offer the services and the technology (Information Technology) that is needed to deliver the services.

Human resources play a major role in delivering services to customers. Customers evaluate the quality of services by comparing the expected level of quality and the actual quality delivered by an employee. Studies show that the higher the job satisfaction is among employees, the higher the level of quality provided and vice versa.

Service quality includes both core services and facilitating services; Barclays Bank's core service is to provide customers with bank accounts and other financial services. Their facilitating services include offering bank cards such as credit cards, debit cards and so on. These facilitating services enhance value of the core services provided by the Bank.

Information Technology incorporates computing, communication, data processing and various other means of converting data into useful information. Intelligent use of information technology not only leads to improved quality and productivity but also gives organizations a competitive advantage. Every service industry is exploiting information technology to improve customer services.

While information technology reduces labour intensity and increases the speed of services, it can have adverse effect on the other dimensions of quality. It may be argued that customer satisfaction is decreased when there is less personal interaction. Thus, service providers must balance conflicting quality concerns. (Bhat 2010, 40).

Phase	**Activity**	**Department having primary responsibility**	**Department having contributory responsibility**
Concept	1. Market research to study user needs and preferences. 2. Analysis of customer complaints of existing product.	Marketing Quality Control	R&D Marketing

	3. Study of competitive product quality. 4. Formulation of qualitative requirements of the new product.	R&D R&D	Quality Control Marketing, Quality Control
Development	1. Review of prototype design and value analysis to see that it meets user's requirement at minimum cost. 2. Qualification testing of prototype to assess its functional efficiency, reliability and maintainability. 3. Review of manufacturing drawings for producibility, interchangeability of components and standardization.	R&D Quality Control Process Engineering	Quality Control, Marketing R&D R&D, Quality Control
Process planning	1. Process planning and conduct of process capability studies. 2. Design and tooling and process control instrumentation. 3. Formulation of quality standards for complete equipment and assemblies. 4. Preparation of procurement specification for materials and bought out components. 5. Formulation of inspection procedures.	-do- -do- -do- -do- Quality Control	Production, Quality Control -do- Quality Control, R&D Purchase, R&D Production, Process Engineering

	6. Design/procurement of special test equipment.	-do-	-do-
Material procurement	1. Capacity verification of vendors. 2. Incorporation of quality requirements in purchase orders. 3. Investigation of defects and causes of out of control process. 4. Analysis of quality data for improvement in the process products.	Purchase -do- Quality Control -do-	Quality Control -do- Purchase -do-
Production	1. Operation of process control and data feedback for improvement. 2. Process surveillance and inspection/testing of product. 3. Investigation of defects and causes of out of control process. 4. Analysis of quality data for improvement in the processed products.	Production Quality Control -do- -do-	Process Engg. and Quality Control Production Production and Process Engg. Production, Process Engg. and R&D

Usage and maintenance	1. Technical advice for proper operation and maintenance. 2. Performance feed back on reliability. 3. Failure analysis.	Market-ing/Service Marketing Quality Control	- Quality Control Process Engg., R&D and Production.

TABLE 1. Quality Activities in an organization (Lal, 8-9).

3.2. International Organization for Standardization (ISO) – 9000

The International Organization for Standardization (ISO) was introduced in 1946. Its aim is to develop a uniform set of international quality standards. As of 2007, it had 158 members representing different countries. ISO-9000 series of standards were published in 1987. Originally, they were designed for the manufacturing sector but were later revised so that these could be applied to any organization. ISO-9000 is a family of standards which defines a quality management system that can assist organizations in enhancing customer satisfaction. It can also provide confidence to customers that the products supplied will meet their specified requirements.

A Quality Management System (QMS) based on these standards can serve as a framework for establishing and institutionalizing quality management in the Bank. Quality management systems based on these standards are designed to continuously improve the performance of the Bank while addressing the needs of its customers and all its stakeholders.

3.2.1 Importance of ISO- 9000 standards for developing countries

Historically, most developing countries had controlled economies with very little competition. Imports were highly restricted and as such, manufacturing companies had captive markets. The major emphasis was on maximizing production to increase profits. Given these conditions, quality was compromised, thereby preventing exporting of products because of poor quality.

ISO-9000 standards can serve as a good framework for organized quality improvements in companies located in developing countries. Furthermore, with the certification these companies can change their poor-quality-supplier image.

Governments of developing countries have also realized the importance of ISO-9000 standards in their export efforts, and are strongly promoting these standards through awareness seminars and other financial incentives such as subsidizing certification expenses.

Unfortunately, while companies have benefited from ISO-9000 certification, there is a tendency, particularly among small and medium companies, to use the certification primarily as a marketing tool. Such companies, with the help of consultants, make just enough compliance efforts to obtain certification, without making any serious effort to use the standards for their intended purpose. What such companies do not realize is that they need to maintain these quality standards in order to ensure that customers are satisfied so that they can receive the certification repeatedly. (Lal, 136-137).

3.2.2 ISO-9000 and TQM

ISO-9000 is not an alternative to TQM, but is rather an important tool for embedding TQM in an organization. ISO-9000 helps to standardize the best practices in organizations; it directly covers issues to do productivity, cost competitiveness and business results. However, it fails to address employee satisfaction and corporate social responsibility. ISO-9000 also makes it difficult for anyone to take shortcuts with the quality of products or services. TQM on the other hand, remains the overall philosophy for wider aspects of quality management and organizational excellence. (Lal 2008, 140).

ISO-9000 Quality Management Principles

There are eight Quality Management Principles in ISO-9000 which lay down the basis for a quality management system. These principles have been derived from the teachings of various quality gurus and were standardized based on extensive discussions within the ISO Technical Committee. They are: (Lal 2008, 129-131).

Customer Focus:

Customers are the sole reason for the existence of companies. Barclays Bank needs to understand current and future customer needs, and should strive to meet customer requirements and exceed their expectations.

The prime requirement for majority of customers is the assurance that their money is in safe hands while at Barclays Bank. With the growing trend of fraud in the banking industry in Kenya, Barclays Bank cannot afford to be complacent when it comes to fighting fraud. The Bank needs to be on the forefront in fraud prevention by utilizing the findings of this thesis and training employees, customers and other stake holders on fraud prevention.

Leadership:

Top management establish the vision and mission for companies. It is also their responsibility to create and maintain an internal environment in which employees feel motivated to achieve the objectives of the organization.

Top management and executives have a duty to ensure that they act ethically at all times. This is the how subordinate employees will learn that the Bank has a Code of Conduct that is upheld and should be respected by everybody working for Barclays Bank of Kenya.

A good work environment where people respect each other and respect the rules provides confidence to employees that they are working in the right organization.

Involvement of people:

All employees are the essence of an organization and their full involvement enables their abilities to be used for the organization's benefit. Many people feel motivated to work and do a good job when their efforts and opinions are appreciated.

Training employees in their specific job responsibilities ensures that they know what is expected of them and can perform more effectively. In case queries arise during their work, employees should be provided with guidance on how to carry out the tasks at

hand. Employees should be treated fairly and the weak ones should be helped to improve their performance instead of being victimized.

Process approach:

A desired result is achieved more efficiently when activities and related resources are managed as a process.

Processes carried out in different departments of the Bank are cross-functional therefore improving the quality in the processes and activities carried out will have a direct positive impact on the Bank as a whole.

System approach to management:

Inter-related processes in the Bank should be identified, understood and managed as a system in order to contribute to the Bank's effectiveness and efficiency in achieving its objectives.

Continual improvement:

Continual improvement of the Bank's overall performance should be a permanent objective of the Bank. In today's competitive market, even the most popular brands and organizations need to constantly develop their brands and revise their strategies. Brand development includes improvement of quality features and usability and reliability of products.

Factual approach to decision-making:

Effective decisions are based on the analysis of factual information. Bank managers need to obtain all the facts on fraud in the Bank, analyse the information and use it to make decisions on how to fight fraud in the Bank. By reducing fraud to the minimum, the Bank will reassure its customers and stakeholders that their investments in the Bank are safe.

Mutually beneficial supplier relationships:

An organization and its suppliers are inter-dependent and a mutually beneficial relationship enhances the ability of both to create value. In the quest for improving quality, the Bank needs to establish relationships with suppliers who offer high quality products and services and adhere to the Bank's specifications. In return, the Bank should ensure that suppliers are treated fairly and are chosen on merit of competitive bidding. Giving favourable treatment to some suppliers over others should be prohibited as it can facilitate fraud.

4 BARCLAYS BANK OF KENYA LIMITED (BBK)

4.1 Introduction to case study

Barclays Bank of Kenya Limited is a subsidiary of Barclays Plc UK. It is one of the biggest banks in Kenya. Barclays has operated in Kenya for over 90 years and has an extensive network of 117 outlets with over 230 ATMs spread across the country. The Bank's financial performance over the years has built confidence among shareholders, with a reputation as one of the leading blue chip companies on the Nairobi Stock Exchange.
Its headquarters are located in the capital city of Kenya, Nairobi in Barclays Plaza. Barclays Bank of Kenya has four business units namely retail (consumer) banking, corporate banking, treasury and card services.

Fraud in banking is defined by law as the criminal offense of knowingly executing or attempting to execute a scheme to defraud a financial institution or to obtain property owned by or under the control of a financial institution by means of false or fraudulent pretenses, representations, or promises.

The purpose of this thesis is to find out why, despite having a Fraud Policy in place, there is a growing trend of fraudulent activities being committed in Barclays Bank of Kenya and find ways to minimize the frauds.

4.2 Fraud

According to CIMA 2009, fraud is defined as using deception to make a personal gain dishonestly for oneself and/or create a loss for another. Any person is capable of committing fraud; defrauding an organization is not an accident but rather a calculated and deliberate act of deception. Fraud does not only involve theft of money but also confidential information and assets.

The Association of Certified Fraud Examiners (ACFE 2002– 2008) conducted a research in the US across a wide range of industries and the results repeatedly indicated that:

- fraud is a widespread problem that affects practically every organisation
- & that the typical organisation loses 5–7 per cent of its annual revenues to fraud.

(Samociuk et al. 2010, 11).

Companies have systems in place to help ensure that transactions are recorded accurately and that proper procedures are followed. They also have policies to guide employees to act in an ethical manner. These systems, procedures, and policies often work to catch errors and honest mistakes in the work process. However, a fraudulent employee deliberately tries to thwart these systems and policies while at the same time attempting to conceal his or her actions.

Some companies have inadequate or nonexistent systems to ensure accurate records of transactions are kept. As such, it becomes very difficult to prevent, detect, and stop fraud from within.

As organizations strive to expand their business processes, it creates a system where management is face with the difficult task of supervising many people at a time, making it impossible for managers to follow all their employee's actions to the letter. This makes it fairly easy for employees to commit fraud because they are entrusted with information and have to access to systems and assets. Employees naturally become well educated on the inner workings of a company and know where the gaps and weaknesses are. (Coenen 2008, 20).

According to Pickett (2007, 11) many top managers view fraud as taboo and a rather boring subject, preferring not talk about it at all. This is because investigating fraud means exposing weak controls and even possibly could lead to reputational damage for the organization. It also means going back to analyze previous company information in order to collect evidence, which often requires a lot of time and money. In many cases, it is difficult to successfully prosecute fraudsters which is why many organizations often resort to laying off fraudulent employees and continuing with business as usual.

4.2.1 Who commits fraud?

Figure 2 shows the potential people or organizations that commit fraud against Barclays Bank. Fraud can be categorized in two broad groups, namely, internal and external fraud. Internal fraud is committed by employees and managers of an organization, either acting alone or in groups or through collusion with outside parties. Collusion between employees dramatically increases the length of time a fraud scheme will go on as well as the monetary value experienced by the company.

Management fraud can be quite difficult to detect because managers have access to most information and systems and have the power to disguise their actions because they know that their decisions may not necessarily be questioned by others. They can also intimidate junior employees to commit fraud on their behalf.

External fraud is committed by third parties of organizations such as suppliers, competitors, partners and customers. Other offenders include potential customers, governments and criminal organizations.

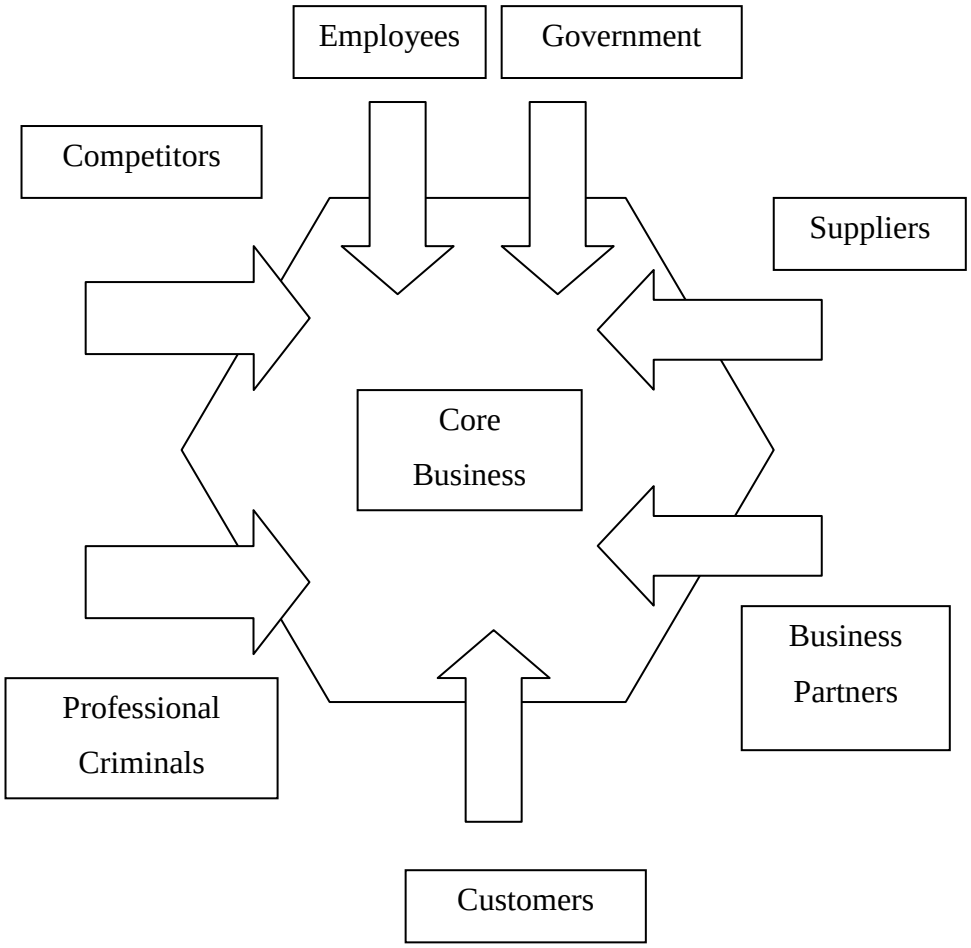

FIGURE 2. Who commits fraud?

Unfortunately, it is very difficult to create a personality of a typical fraudster simply because people have very different personalities and reasons for committing fraud. However, research by psychiatrists has identified one personality type which seems to have a much higher motivation to commit fraud; a person with this type of personality is known as the 'corporate psychopath'. A Canadian psychologist, Dr. Robert Hare, identified the following eight traits to try to define a corporate psychopath:

- glib and superficially charming (a smooth talker but unfortunately is insincere making it quite difficult for the other person to tell if what is said is true or not.)
- grandiose sense of self-worth (makes a strong impression on others with his/her personality.)

- pathological liar (a seasoned liar with a great capacity to exaggerate or twist the truth quite skillfully.)
- very skilful manipulator (can trick others in order to obtain personal gain.)
- lack of remorse (shows no pity or guilt even when on the wrong.)
- displays shallow emotions
- callous and lacks empathy
- fails to accept responsibility for his/her own actions.

Individuals with these traits can reach the highest levels in an organisation and can wreak untold damage. Interestingly, there is very little to distinguish this type of person from the rest of the people in society. Hare emphasizes that a person displaying some of these characteristics is not necessarily a corporate psychopath.

Corporate psychopaths have an overwhelming urge to obtain the power and status that having a lot of money brings. They desire influence and power over their colleagues, make plans over long periods of time, and are able to lie, deceive and manipulate as required without feeling any remorse. People with psychopathic traits have no qualms about manipulating honest employees.

A survey in 2006 indicated that 92% of people who commit fraud have no prior criminal charges or convictions related to fraud. This, however, does not mean that companies should stop carrying out prior criminal checks before hiring new employees. (Coenen 2008, 27).

Men and women commit a fairly equal number of frauds at work. The most recent ACFE survey indicated that 61% of fraud schemes were perpetrated by men, while 39% were committed by women. The study notes however, that fraud committed by men is much more costly. (Coenen 2008, 28).

4.2.2 Why commit fraud?

Dr. Donald R. Cressly invented the Fraud Triangle that explains how the process of fraud occurs. The Fraud Triangle consists of three levels that a dishonest individual or group goes through in order to commit fraud:

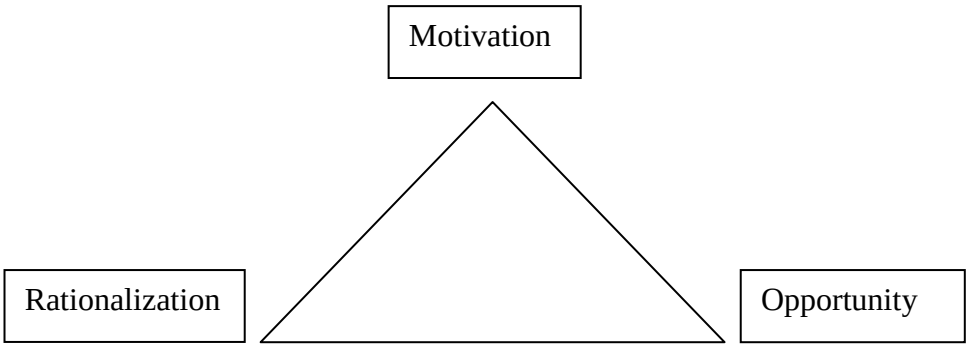

FIGURE 3. The Fraud Triangle

Motivation refers to the pressure or need that an individual feels in order to commit fraud. It could be a true financial need such as outstanding bills or personal debts or could also be a perceived financial need which one is unable to satisfy with his/her current income such as expensive holidays and cars, gambling or even drug addiction.

Motivation can be constrained by management, although not to the degree that opportunity can be limited. The best way to reduce ‘‘needs’’ is by paying employees fairly (to reduce perceived financial burdens) and by creating performance systems that are reasonable (not requiring job performance beyond what is realistic).

Opportunity to commit fraud refers to access of assets, information or money. The perpetrator usually uses his/her position or relations with the organization to either override systems, forge documents or dupe honest employees in order to gain the perceived reward, without getting caught.

Management has the most control over the opportunity portion of the fraud triangle. It can limit access to assets and put controls in place that ensure monitoring of systems and people.

Rationalization refers to the process of justification of the fraud by the individual. This is determined by the morals of an individual; moral standards differ among individuals and across cultures. This is the most dangerous level because it is impossible for organizations to control the minds of employees. (Coenen 2008, 13).

4.2.3 Internal Fraud

Research shows that internal fraud is committed by both employees and management and accounts for 50-80% of frauds committed in organizations. Employees have access to information, processes, systems and assets therefore making it easier for them to device ways of committing fraud without being detected. (Goldmann 2009, 12).

The Bank's statistics show that the frequency of internal fraud is increasing drastically and has by far inflicted the most significant losses to the bank. This is because some dishonest employees and managers have found ways to override systems and or collude with outsiders to defraud the bank. According to the Bank's fraud unit, management fraud occurs less frequently but accounts for the greatest financial losses. Position equals power; managers and executives, having more access to more information and assets than regular employees and can commit fraud relatively easier without being noticed.

Table 2 shows the different types of internal fraud identified by the Bank and their impacts on the Bank. The risk size represents the amount of money that the Bank stands to lose to the specific type of fraud. The probability of occurrence represents the number of fraudulent cases that are witnessed by the Bank annually. A scale of 1 to 5 was used to create the table, 1 being the least and 5 being the highest value. The impact on the Bank was determined by multiplying the risk size and the probability of occurrence. A detailed explanation of the table is offered under each type of fraud.

Type of fraud	**Risk size**	**Probability of occurrence**	**Impact on the Bank**
Cheque fraud & fund transfers	4	2	8
Bribery & conflicts of interest	4	2	8
T&E claims	3	2	6
Theft of confidential information	5	1	5
Misuse of assets	1	3	3

TABLE 2. Internal fraud risk chart

Cheque fraud and fund transfers

Although is it relatively easy to get caught, some employees opt to steal cheques that have already been signed and prepared for delivery and alter the details of the cheques, either manually or electronically. The altered cheques are then cashed by the employees themselves or given to outsiders to cash them.

Another method that has been used by employees is to hide fraudulent cheques among a pile of genuine cheques. The person in charge of signing the cheques is usually quite busy and may not have the time to go through the details of each cheque thoroughly. The person then signs the cheques and authorizes them to be released. The fraudster outsmarts the signer by exploiting the individual's inattentiveness to the details of the cheques.

Some other dishonest employees have devised ways of transferring relatively large sums of money from dormant accounts containing huge sums of money to bogus accounts that were created earlier using fake documents. They choose to transfer funds from dormant accounts because they know that it will take some time before anybody notices that something weird is going on. Transferring funds to bogus accounts ensures that the fraudulent activities cannot be traced back to them, in case they are discovered.

The Bank notes that the frequency of these types of fraud occurring is not so high, but their impact on the Bank is extremely high because very large sums of money have in the past been lost through such fraudulent acts. As such, these types of fraud need to be looked into immediately and ways to reduce them determined as soon as possible.

Bribery and conflicts of interest

Bribery is the most basic form of corruption and includes accepting gifts or bribes from suppliers, customers and potential business associates in order to gain favour. Bribery can also be in the form of giving or accepting bribes from government officials to 'get things done.' This type of fraud is mostly perpetrated by managers because they are in

powerful positions and are responsible in making decisions regarding potential suppliers and partners.

Conflicts of interest exist when an employee or manager also has a direct but secret financial interest in a company that does business with an organization, such as a construction firm, equipment leasing company, payroll service, or any other outside vendor. A conflict can also exist where a spouse or friend of the manager receives favoured treatment in bidding for contracts.

These types of fraud do not occur so regularly, according to the Bank's statistics. However, their consequences are dire. Not only does the Bank lose a lot of money and assets but also has its reputation badly damaged because such cases of fraud usually reach the media. Some reported cases include awarding contracts to private companies linked to bank managers' families or friends to provide consultative and training services for employees.

Travel and entertainment (T&E) fraud

This type of fraud is usually favoured by employees with expense accounts. In fact, it is categorized as among the costliest forms of internal fraud in many organizations. Part of the reason is that it is generally very easy to get away with these schemes because implementing effective preventive controls continues to prove very difficult, in no small measure due to the virtually limitless number of ways that these frauds can be perpetrated. (Goldmann 2009, 39).

Bank records show that some employees falsify receipts of purchased goods and services in order to receive compensation for the costs incurred. Others have been known to submit multiple expense claims in order to be compensated more than once. Other cases include falsifying car mileage expenses and falsifying approvals of travel expense claims.

Due to the fact that only managers and few employees in the Bank have the rights to expense accounts, this type of fraud does not occur so frequently. In the cases that have been discovered however, the amount of money that was lost was considerably high, making it a high risk fraud which should be acted upon immediately.

Theft of confidential information and abuse of computer systems & processes

Employees have access to information, processes, systems and controls and can exploit computer control weaknesses in organizations to access and steal confidential information. Customers and shareholders may lose confidence in management's ability to secure the organization's sensitive information.

These types of fraud are especially common in Kenya where Bank employees collude with outsiders to rob Banks of their money during transportation. Bank employees have been known to divulge information to armed gangsters on the time, place and route that security vehicles delivering money to certain destinations will use. Armed gangsters then hijack the security vans and make away with millions of Kenya shillings, which in most times, is usually not recovered.

Some employees have also been known to use computer systems to steal money via fraudulent funds transfer or manipulate computerized processes in order to gain access to confidential information. Gathering of information can be done through hacking where employees with exceptional computer skills break into the Bank's computer systems. Another way is through social engineering where fraudsters persuade staff that they "need" or "have special permission" to access secure areas of the organization's computer systems.

Barclays Bank reports that it is yet to experience a case of fraud where employees collude with gangsters to intercept security vehicles carrying loads of cash. However, statistics show that the Bank has from time to time experienced cases where employees have deliberately hacked into computer systems and downloaded vital information such as customer account numbers and other details.

Misuse of organization owned assets

Even though this type of fraud is considered minor because it costs organizations little or no cash, it has become a common occurrence in the bank and is unacceptable. Such types of fraud include misusing company cars, telephones, computers, stationery and

software. Majority of employees in the Bank are known to use resources such as telephones and stationery for personal benefit.

4.2.4 External Fraud

External fraud is committed by people outside the organization. The perpetrators can work independently or can collude with staff to defraud the Bank. The various types of external fraud witnessed by the bank are:

Type of fraud	**Risk size**	**Probability of occurrence**	**Impact on the Bank**
Money Laundering	4	2	8
Identity theft & use of lost or stolen documents	2	3	6
Use of counterfeit cards	2	3	6
Theft of confidential information	5	1	5

TABLE 3. External fraud risk chart

Identity theft and use of stolen or lost documents

According to Biegelman (2009, 29) this is the most common and fastest –growing financial crime worldwide. Criminals acquire personal identifying information such as name, address, date of birth, Social Security Numbers, identification cards, credit information, and other vital details in order to impersonate and defraud the victim. In Kenya, unfortunately, forging of Identity cards and other documents is fairly common which facilitates identity theft.

Barclays Bank of Kenya continues to be a victim of fraud through identity theft. It is very easy for criminals to get hold of a victim's personal information. They could obtain it from the mail, the internet, retrieving documents from the dumpster, stealing documents from office desks, and so on. The perpetrator then uses this information to assume the victim's identity. Once the imposter has the necessary documents, it is then

very easy for him/her to present them to the bank to either open accounts, obtain credit facilities or to withdraw money from the victim's account.
Very many incidents of fraudsters using stolen or lost documents and cards are witnessed by the Bank annually. Sometimes the loss of documents and payment cards through misfortune or theft goes unnoticed for long periods of time. It becomes very easy for fraudsters to use the stolen or lost documents without detection.

These types of fraud can be relatively costly if not detected quickly. However, the Bank notes that since withdrawing huge sums of money at a time require some strict procedures, and the fact that one can only withdraw a specific amount of money via the ATM a day, many fraudsters chose to withdraw and spend relatively lower amounts of money to avoid quick detection.

The acts of conning innocent people and pick pocketing are very common in Kenya, especially in the capital city. Con-artists and pick-pockets have mastered their skills over the years without the possibility of alerting their victims and or being caught. These acts of stealing account for majority of lost documents for instance IDs and payment cards.

Use of counterfeit cards

The use of debit and credit cards as a means of payment has grown tremendously over the years. Debit and credit cards are made of plastic and are embossed with information such as the card number, the expiration date and the cardholder's name.

Data can be encoded and recorded on a single magnetic stripe that is applied on the back side of the card or it can also be stored in a chip where information is stored in the permanent memory of a microprocessor chip embedded in the card. The greatest cause of concern with the continued use of the magnetic stripe technology is the increase of abuses reported worldwide. Attackers have great insight about the design details of magnetic stripe cards, which helps them to identify security weaknesses that could lead to fraud. In face-to-face payment transactions, counterfeiting the magnetic stripe has become a dangerous threat. (Radu 2002, 54).

PICTURE 1. A magnetic stripe card (Photo: HIWTC 1998-2011)

PICTURE 2. A chip card (Photo: MasterCard 1994-2011)

A fraudster can acquire the details of his/her victim's card by eavesdropping. This refers to dishonest access of financial data, which is either embossed on the card or stored on the magnetic stripe of the card.

There are several ways in which eavesdropping can occur:

It is common in the restaurant industry for a waiter to access a card holder's information by quickly jotting down the financial data embossed on the card. This has come to be known as the *waiter attack*. When a waiter takes the victim's card to make the payment at the cash register, he can quickly write down the information on the card and use it to produce a counterfeit card in the victim's name. This is possible to carry out with magnetic stripe cards.

A fake ATM or POS terminal under the control of the attacker is used to illegitimately read the financial data encoded on the magnetic stripe of the card. These are small handheld devices which are the size of a matchbox and can also be attached to ATM terminals and can read the magnetic stripe of a card in few seconds: These devices can store information of up to 50 cards at a time, which is later transferred to the logistic department of a criminal organization and used to create the counterfeit magnetic stripe cards. (Radu 2002, 25).

Lack of reliable cardholder verification procedures usually facilitates the possibility of fraud. An attacker who uses a counterfeit payment card impersonates the authorized cardholder by attempting to use the card for his own convenience. (Radu 2002, 25).

"A new wave of theft using automated teller machines is sweeping through the country, leading to the loss of customer savings daily. So widespread is the crime that police and banks appear helpless on how to contain it.

The number of complaints reported to various banks and police is on the rise, according to records seen by the Saturday Nation.

On Thursday, two Bulgarians, Ivan Petkov and Milko Kostadinov, were arrested and charged in a Kilifi court when they were found with 44 ATM cards and over Sh2 million.

The money is believed to have been stolen from various bank accounts using the cards.

Further investigations revealed that the two had stolen the money belonging to a commercial bank in Meru.

Last week, several customers of the bank lost their money through ATM withdrawals." (Angira 2011, 1).

"In one case in Meru, the fraudsters used a replica of the ATM card made with a simple electronic gadget that writes information to blank cards.

The other theft is through what is called card skimming. This involves the capturing of data from the magnetic strip on the back of an ATM card.

Skimmers are small and are often fastened near the ATM's factory-installed card reader, and they can capture information such as the account number, balance, and PIN number from up to 200 used cards." (Angira 2011, 3).

Many banks in developing countries issue their customers with the magnetic stripe cards. The reason that the magnetic stripe card is still mainly used is because majority of banks have not installed the chip technology due to its high cost of installation and maintenance.

Barclays Bank of Kenya is of no exception when it comes to fraud committed through use of counterfeit cards. The number of cases witnessed by the bank through this type of fraud is overwhelming. In fact, fraud investigators have handled several hundreds of cases related to use of counterfeit cards this year. This fraud costs the Bank relatively large amounts of money because it has to compensate victims of the fraud. A lot of attention has to be focused on this type of fraud and action taken immediately.

Theft of confidential information

This type of fraud occurs when fraudsters hack into a company's computer systems and steal confidential information. They can then use this information to steal customer or vendor identities or to extort the organization. (Goldmann 2009, 113).

Though this type of fraud is not very common, though it has been witnessed on a few occasions where an ex-employee or a criminal gang has hacked into the Bank's computer systems and downloaded vital information such as customer information, their card numbers and so on. It is very difficult to estimate the monetary value of this type of fraud. However, if it occurs, it costs the bank so highly because the Bank risks losing valuable information to its competitors, criminals and the public at large.

Money laundering

Money laundering is the means used to convert funds that proceed from illegal activities such as sale of drugs into financial uses that involve legal instruments, for example bank deposits, investments in stocks or real estate. (Grosse 2001, 3).

Barclays Bank of Kenya faces challenges of dealing with money laundered from drugs, corruption, pirate activities, and so on. Unfortunately for the bank, it is very difficult to determine where the money comes from because criminal gangs are very intelligent and have devised ways of disguising their wrong doings.

The possibility that the Bank could unknowingly be transacting with criminal gangs is very challenging. If for instance such a transaction was to come in the limelight, the Bank could face a catastrophic damage to its reputation and customer confidence.

5 ENTERPRISE RISK MANAGEMENT (ERM)

Enterprise risk management is the process of identifying major risks that confront an organization, forecasting the significance of those risks in business processes, addressing the risks in a systematic and coordinated plan, implementing the plan, and holding key individuals responsible for managing critical risks within the scope of their responsibilities.

By identifying risks and implementing plans to manage these risks, organizations eliminate the threat of losing business to their competitors. ERM also provides stability in creating, distributing, financing, and selling products and services. Finally, it adds to confidence that the Board and CEO are meeting fiduciary, community, social, and ethical responsibilities and helps build good relationships with regulators. (Hampton 2009, 18-19).

A major rationale for ERM is that it is better to deal with risk in terms of prevention than in terms of recovery. The ERM goal is to develop information systems that identify risk and share the findings. Then, the entity can seek to provide structural incentives for individuals who are ahead of their time to mitigate exposures not seen by others. (Hampton 2009, 45).

For the purpose of this study, we shall look at ERM with an emphasis on fraud.

The fraud risk management strategy

Operating in business is a risk in itself because it makes organizations prone to fraud. A fraud risk is the chance of a perpetrator(s) committing a fraud which has an impact on the organisation. A fraud risk management strategy helps to predict, pre-empt and prevent fraud; it is an important way of adding value and effectively governing an organisation. It is designed to assist executives to develop an organisation that resists fraud in ways that are readily measured and are comparable to other organisations.

The risk posed by fraud comprises three elements:

- the method used to commit the fraud
- the effectiveness of anti-fraud controls systems
- the degree of dishonesty and skill level of the perpetrator

Increasing pressure from national and international legislative bodies requires organisations to implement a fraud risk management strategy. Many organisations already have a fraud risk management strategy in place but unfortunately, are unable to utilize it to its full capability. (Samociuk et al. 2010, 3, 6).

A ‘zero tolerance’ policy is the optimum standard for all organizations that are committed to fighting fraud. However, it is not always easy to implement. This is sometimes due to the fact that the loss inflicted on the organization by the fraudulent act may be significantly less than the actual investigation. It may also be that the amount of time spent investigating the fraud may force employees to divert their attention from their normal work in order to deal with the issue, which could carry on for a long time. This is the reason why an effective fraud management plan calls for preventative rather than curative measures against fraud. (Samociuk et al. 2010, 12).

Independent studies conducted by KPMG and Ernst & Young in 2006 indicated that fraud risk management is becoming more important to companies, and it is of increased importance when companies engage in strategic planning. Organizations that implement company-wide fraud awareness training cut fraud losses by 52%. The study further indicates that companies are devoting more time and resources to fraud management, with

the focus generally on fraud detection and reporting. However, less emphasis is being placed on fraud prevention and responses to the discovery of fraud. (Coenen 2008, 5).

5.1 Developing a Fraud Management Plan for Barclays Bank of Kenya

If Barclays Bank of Kenya wishes to implement an effective fraud management strategy, it needs to look at the previous cases of fraud, both internal and external, and then create a list of the major elements that should be put in place to reduce risks of similar events reoccurring.

There are several factors that could have enhanced the possibility of fraud occurring in Barclays Bank of Kenya:

- the fraud risks are not fully understood
- management involvement in fraud management & supervision is poor
- weak internal controls systems
- red flags and fraud warnings being ignored
- assumptions made that every employee is honest and is incapable of committing fraud

The top management and Board of Directors of the Barclays Bank of Kenya need to support the strategy fully and should involve the whole organization in the project.
To ensure that the Board fully supports the strategy, the following should be observed:

- The real cost of fraud (monetary & reputational damage to the Bank and loss of customers) should be communicated.
- That all employees adhere to the Code of Business Conduct of the Bank. Simply because people look innocent, they should not be allowed to set their own level of honesty at work as it may be out of step with what the employer expects.
- That motivation to commit fraud varies from person to person, and is influenced by time and circumstances.

The identification and reduction of fraud should be treated separately in the Bank’s overall risk management strategy.

According to Samociuk et al. (2010, 8) there are six steps that the Bank should follow in order to develop a fraud risk management strategy:

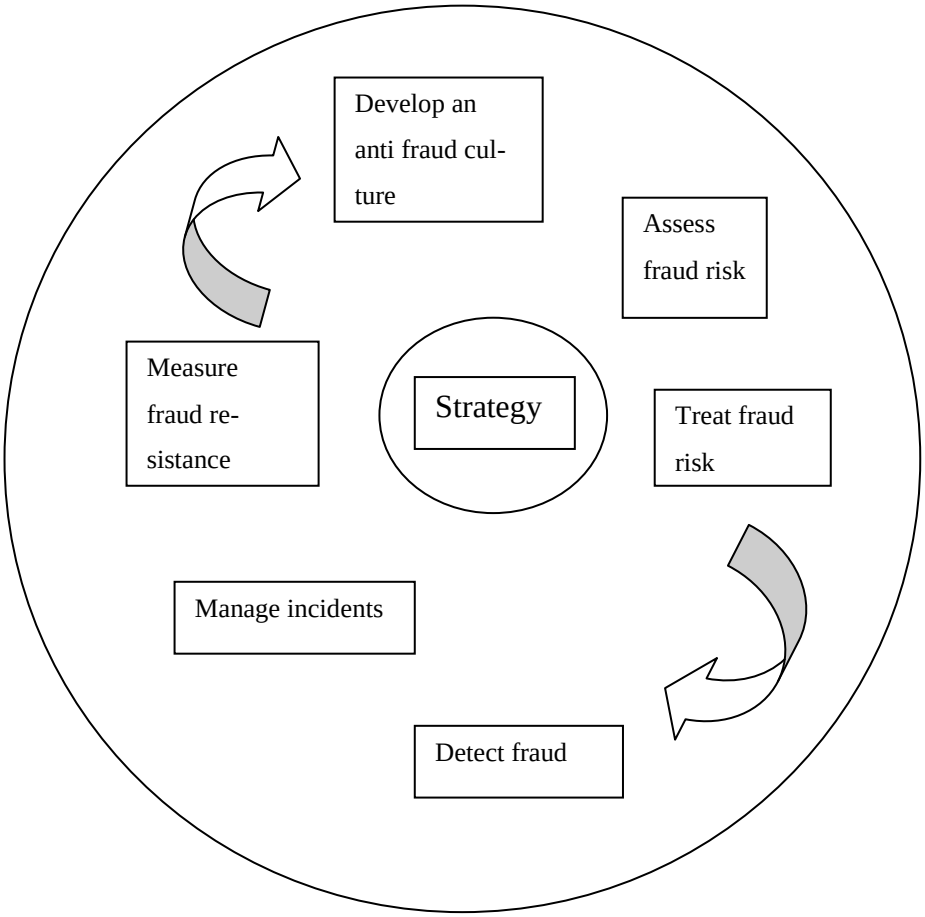

FIGURE 4. The six-step fraud risk management strategy

5.2.1 Developing an Anti Fraud Culture

Organisational or corporate culture refers to the unique way that each organization goes about doing its business. Corporate culture includes shared values, norms, beliefs and ethical practices which make up the character of the organisation.

The top management of Barclays Bank of Kenya need to emphasize the importance of fraud risk management as a way of adding value to the Bank and for effective governance of the Bank.

The Bank's Policies covering business ethics and fraud should be fully communicated and supported across the organization. Other stakeholders of the Bank also need to be informed of the policies, the Bank's stand on fraud and actions taken against fraudsters. The appropriate individuals need to be determined and assigned roles and responsibilities for implementing the fraud risk management strategy.

Domineering executives who are ruthless and aggressive risk takers fixated on profit can act as potential barriers to developing an anti-fraud culture. While nothing is wrong with this approach, these executives may begin to bill their personal expenses to company accounts or use employees to run their personal errands for them simply because they are making large profits for the company. They most likely may not even see it as fraud. However, despite being invaluable assets of the Bank, such actions should not be tolerated under any circumstances. (Samociuk et al. 2010, 29-47).

5.2.2 Assessing Fraud Risk

Fraud risk assessments should be engaging and motivating. The chosen risk assessment team should be assigned a leader who will take up the role of fraud analyst to come up with ways of improving the existing fraud management plan.

Fraud risks should be analysed based on 'likelihood' and 'consequence' and then rated in a way which allows management to prioritise them and decide whether or not they are willing to tolerate them. After identifying the methods and associated controls, treatment options can then be identified.

The Assessment Process

Step 1: Collecting background information

Prior to beginning the process of collecting information, top management of the Bank needs to inform participants of the assessment and encourage them to participate actively. The appointed team should collect information that will provide a good understanding of the Bank; its products & services, strategies, previous years' results, audit

reports, policies, organization charts, processes, business environment, partners and customers.

As mentioned earlier in the report, the current fraud risk assessment team of the Bank has identified the following methods that have or continue to be used to commit fraud:

- cheque fraud and fund transfers
- bribery and conflict of interest
- travel and entertainment fraud
- theft of confidential information
- misuse of assets
- identity theft and use of stolen and or lost documents
- use of counterfeit cards
- money Laundering

Researching high-value frauds that may have occurred in other banks may help identify other potential fraud methods.

Only employees who have hands-on knowledge of how things work should be interviewed. These are often team leaders, supervisors and line managers. Senior managers and executives should be interviewed about potential fraud risks in their job functions, but are not usually involved in creating methods and potential worst-case scenarios for their team. This is because once senior managers realise the scale of potential losses which could occur in their departments, some can become defensive and try cover-up some information.

The assessment team should seek to understand the methods of fraud applicable to each job function and external relationship. This approach is advantageous in that not only does it assess risks, but also helps to understand the level of awareness of among employees.

The team encourages employees to ‘think like thieves’ by urging them to avoid concentrating on existing controls which they believe to be strong but instead to think about how they could be bypassed. This approach has been questioned because it seems to

encourage employees to commit fraud. However, it has been found to yield ideas that have consequently led to fraud prevention.

There is a risk that a dishonest person could participate in a risk assessment. Luckily, one of the aims of the fraud risk assessment is to make dishonest people aware of the fact that they are being watched by others who are alert to fraud risks.

Wherever possible, for the fraud risks identified, additional controls should be put in place; however, segregation of knowledge on the monitoring and detection controls acts a good preventative measure.

The Bank should repeat this fraud risk assessment periodically rather than being a one-off exercise. In case of changes in computer systems, new product/service release or venturing into a new market, updates should be made on the risk plan at hand. Managers should then report to the Board whenever such changes produce unacceptable fraud risks.

Step 2: Knowledge Transfer

The best way to raise awareness about how fraudsters manipulate people is by using actual examples. The assessment team can use real case studies that have occurred earlier in the Bank as a way to communicate the message to employees. They could also pass around real forged documents that have been seized in order to awaken employees' and managers' thoughts and feelings toward fraud prevention.

One aim of the knowledge transfer exercise is for employees to recognise how a seemingly secure control actually facilitates fraud because honest employees do not suspect anything unusual.

Another aim of the exercise is to show employees that perceived control weakness does not necessarily translate into a fraud risk; once a way to bypass controls has been identified, a fraudster still has to obtain the benefit. (Samociuk et al. 2010, 49-77).

5.2.3 Treating Fraud Risk

There are four options of treating fraud risks:

Avoiding the risk

Once a fraud risk analysis has been carried out and the risk has been determined to have extreme consequences to the Bank, it should be avoided altogether. An example here could be for the Bank to avoid transacting with a supplier or customer who is suspected of money laundering.

Reducing the likelihood or consequence of fraud

Some risks paused by fraud can be reduced through increased monitoring, implementing stronger internal controls, improved training or better planning. The fraud assessment team at Barclays should ensure that their IT staff has been trained to monitor and respond to suspicious transactions being carried out either by staff and or third parties. Such activities may include downloading huge files, especially those that contain crucial company information, logins at unusual times of the day, using passwords of employees who are on holiday, and so on.

Another way that Barclays Bank can reduce the risk of fraud is by installing the chip card technology, which offers a much safer way for its customers to transact using payments cards. This technology unfortunately does not come cheap, which means that it should be among the strategic decisions that managers should consider.

Transferring the risk

Some fraud risks such as theft of company assets could be avoided by taking out insurance policies on them. It is essential where risk is transferred that principles of fairness and equity are observed.

Retaining the risk

This measure is taken where the risk cannot be avoided, transferred or reduced, or where the cost of doing so cannot be justified. However, managers should be aware of the possible consequences. Since Barclays Bank cannot do away with Travel & Entertainment claims, it can retain the risk but ensure that strict measures are taken to prevent fraud. An example of such a measure could be to select some T&E claims randomly and subject them to audits.

Another measure to that can be taken to reduce T&E fraud is by installing software that generates and processes the T&E claims in order to prevent the submission of multiple claims and or falsification of approved claims.

Once the treatment of fraud risks have been established, employees need to be trained to become aware of fraud, how they can detect fraud before it actually occurs and how to react in case they notice suspicious activities.

Fraud awareness training should be used to remind employees to remain vigilant, especially at times when they might be more susceptible, for example, when they are under pressure to meet cut-off times or to process invoices before close of business year. Employees should be encouraged to report odd-looking or unusual transactions rather than just process them. Practical awareness training increases the potential for all employees to recognise the red flags of fraud and know how to respond to them.

The Bank should also ensure that its business partners and other stakeholders receive a minimum level of fraud awareness training. The Bank should raise customer awareness about the dangers of identity theft, the loss of payment cards and internet banking fraud by providing information on its website and training customer service personnel to inform customers about fraud.

The Bank should strive to maintain a continuous high level of awareness, enforcing key messages through the use of mediums such as posters, articles, newsletters, short films and perception surveys. (Samociuk et al. 2010, 79-101).

5.2.4 Detecting Fraud

Despite the efforts made, it is not possible to prevent or eliminate all frauds which is why it is important to put in place measures to detect fraud. Finding fraud can be one of the most challenging and interesting areas of fraud risk management. Detecting fraud early enough helps to minimise losses and increases the likelihood of recovery for frauds that have been identified. Putting detection measures in place can also act as a deterrent, preventing potential frauds from being committed and making the organisation more resilient to fraud.

Training and encouraging employees to recognize, respond to and report the red flags of fraud are two efficient and effective ways of detecting fraud. When training employees to detect fraud, they should be informed that not everybody within or outside the organization is honest and trustworthy. Despite the fact that it is difficult to establish who is honest or not just by looking at them, certain red flags that can help detect fraud or raise suspicion have been established. These red flags are categorized as behavioural, transactional, system or corporate.

Behavioural red flags; objective and subjective

Objective behavioural red flags can be measured and include things such as excessive wealth or overspending, increasing debts, long absences from work or failure to take leave, change of work patterns, staying long in the office after normal work hours and repeated override of normal control procedures.

Subjective behavioural red flags are usually dependent on the manager's knowledge of the employee. It includes problems with gambling or drug use, excessive mood swings, aggression, evasiveness, misleading answers and resistance to answering to audit or routine questions.

Transactional red flags

Information held on computer systems, paper documents and reports can contain transactional red flags in the Bank. Employees working in risk areas such as procurement or payroll should receive specific training in recognising transactional red flags. Some typical ones include:

- ‘ghost’ business partners or suppliers who do not necessarily exist but are just a front for fraudulent activities
- non-transparent counterparties where, through basic open-source research, indications of criminal association exist
- preferential supplier treatment and/or a lack of competitive tendering
- payments made into executive and employee-controlled accounts
- hiding a conflicting ownership interest in suppliers, customers and business partners using a cascade of offshore companies to disguise the ownership
- unusual delivery of instruction, for example through the mail or by courier with an urgent processing request
- photocopied documents or attachments
- unnecessary words or explanations on the instruction to try to make it seem more legitimate
- appearance or style not consistent with the normal, of a business partner or customer
- incorrect beneficiary name, address or account number
- suspicious-looking documents, such as IDs, payment cards and passports; for example, the photograph on the document does not match the person presenting the document

System red flags

The IT department of the Bank can play an important role in monitoring for red flags in computer and communication systems. All employees need to be informed that systems are constantly monitored, but monitoring should be done only by the systems team.

Indicators of irregular behaviour might include:

- controls or audit logs being deliberately turned off
- someone logging into a system using the user identification and password of an employee who is on leave
- a higher than average number of failed logins
- logins at unusual times of the day

- downloading or even sending huge files with company information, especially to unknown recipients

The corporate red flags

Potential corporate red flags which we have regularly led to the fall of organizations include:

- autocratic management decisions around business relationships, such as a refusal to change a major supplier
- losses and declining margins on sales
- artificial barriers put up by directors to avoid answering questions
- overriding of budgetary controls
- incomplete records
- unusual manual transactions and adjustments

Corporate red flags are arguably the most difficult group on which to build a detection programme because they are difficult to interpret. Specialist experience and training may be required.

In case employees notice something suspicious, they should report concerns usually through their line manager or, if it involves their line manager, through a whistle-blowing procedure or help line. Once a concern is reported, it should be followed up. If an employee is brushed off by a manager the first time they try to raise such an issue, it could easily be the last time they raise any issue.

After an incident is reported, evidence should be obtained by examining the details; no assumptions or gut decisions should be made. Red flags may need to be prioritised into areas which should be investigated further, and those which should be put on hold. This is because fraud investigation can be a highly expensive and resource consuming process.

Managers should have some guidance on how to respond to potential incidents of fraud. Guiding instructions could be included in the Fraud Policy or included in a fraud response plan.

There should be close cooperation between support functions, such as human resources, and enforcement or control functions such as security or internal audit, to ensure that follow up and resolution of red flags is consistent across the organisation.

Another common way to detect internal fraud is by accident. About 25% of frauds are detected accidentally. This could be a phone call or email routed to the wrong person, a letter that is inadvertently intercepted, or even from an outside party. Despite all the amounts of resources that are put into fraud prevention, one-fourth of frauds are still discovered by accident. (Coenen 2008, 15).

According to the 2006 study by the ACFE, 34% of frauds are detected through a tip from an employee, vendor, customer, or anonymous person. This is why it is important to have an anonymous hotline available for people to report fraud. The anonymous hotline ensures that people feel safe to report suspicious activities without the possibility of their identities and jobs being revealed. (Coenen 2008, 14).

Performing pre-emptive health checks is highly recommendable for the Bank. These health-checks can identify many of the red flags early on in a potential fraud, prevent it from occurring, or at least stop it, before major costs are incurred or expensive investigations need to be carried out. Also, in an environment where health checks are routinely performed, the likelihood of detection is apparent, creating a strong deterrent to potential fraudsters.

The objectives of a pre-emptive health check vary, depending on the scope of the project, who is conducting it and the nature of the transactions reviewed. Typical objectives of pre-emptive health checks may be to:

- evaluate how the organisation's Code of Conduct is working
- determine whether previously identified fraud risks are occurring in practice
- identify areas which should be focussed on in upcoming internal audit or security reviews
- identify areas of cost saving and revenue enhancement, such as duplicate supplier payments, overbillings, suspicious or inappropriate counterparties

- evaluate the effectiveness of internal controls and how frauds can be prevented

A number of analytical tools and methods are available to detect red flags. The bank can, for example, implement specialist software that automatically detects suspicious credit card transactions.

Another preventative measure that can be taken to prevent fraud in the Bank could be to install software for data mining to detect corporate fraud in, for example, procurement systems. However, using such software should be carefully planned and tightly focussed. Lack of planning and focus can result in an analysis containing many hundreds of red flags which cannot possibly be followed up.

A fraud detection test should analyse data and transactions on computers, indicators related to individuals, documents and information related to third parties such as customers, suppliers and partners. (Samociuk et al. 2010, 103-127).

5.2.5 Managing Incidents

It is the duty of employees to report any incidents. They should also be informed how these incidents are escalated and investigated. Some organisations include this in their Fraud Policy and/ or Fraud response Plan.

A Fraud response Plan ensures that incidents are handled in a systematic and efficient manner, not only to secure a successful investigation, but also to show that the organisation acted in a prudent and lawful manner. It also sends a message that the organisation does not tolerate fraud.

Once a fraud is discovered, a Fraud incident management team should be formed. It usually comprises essential members and co-opted members. Essential members may include:

- the Chief Financial Officer
- the Fraud risk Manager
- the Senior Manager in the affected area
- a designated Project Manager, if appropriate

- a secretary or administrative assistant

Co-opted members will depend on the type of incident and may include a range of technical specialists and service providers, such as:

- internal support departments such as insurance, legal, corporate security
- external lawyers
- police and telecommunications agencies
- forensic service
- investigators

The different response actions to fraud are internal actions or dismissals, civil procedures and criminal prosecution, or a combination of approaches. Whichever action is taken will depend on the Bank and the significance of the fraud. However, it is strictly advised to consider each cause of action thoroughly before implementation especially because the documents may at a later stage, come under the close scrutiny of third parties such as insurance loss adjusters, lawyers and/or regulators, as well as stakeholders such as shareholders.

Objectives of handling a fraud case:

- control the immediate situation as quickly as possible
- continue business operations with minimum disruption and loss, and maintain business confidence
- understand the full extent of the fraud and all the people involved
- clear innocent people from suspicion
- determine why controls failed to prevent the fraud and rectify the situation
- dismiss dishonest employees
- terminate the contracts of colluding third-party suppliers or contractors
- prosecute all of the perpetrators
- recover losses by all available means, including fidelity insurance and civil litigation
- deter employees and third parties from attempting frauds in future

- maintain effective communications internally and with customers, the media and other stakeholders

Collecting evidence of the fraud should be as discrete as possible so as not to alert the potential suspects. All persons who collect information should have the experience and/or technical knowledge to do it in a controlled and legally acceptable manner.

A common mistake is to try to conduct covert and overt actions simultaneously. This can compromise future interviews with suspects and lead to loss of evidence. Examples of covert actions include analysis of expense and telephone records and database research or surveillance to gather evidence. Overt actions include interviews, civil actions and police arrests.

Even after a full investigation, when confronted with proof of their wrongdoing, many fraudsters do not admit liability or accept their punishment without a fight. The fraudsters may use counter attack methods such as:

- adverse media stories about the way in which the investigation was conducted or the techniques which were used to gather evidence
- releasing compromising information about the Bank's business dealings in order to discredit management in the eyes of stakeholders
- spreading malicious rumours within the Bank in order to demoralise employees
- launching their own civil, libel or defamation actions
- threats of violence (although quite rare)

Coenen (2008, 8) explains that another defence mechanism that a fraudster may use when intercepted is to imply that it was simply an error that occurred during business transactions. Sometimes, it could be true because plenty of errors are made daily in business. This is the reason why fraud investigators look for evidence of intent to defraud in the documents and actions of the accused.

Responses about the Bank's ethical stance should be prepared in anticipation of malicious counterclaims, reiterating that all interview methods and investigation techniques are legal, and have been reviewed by legal advisers.

The Bank should include a statement in the Fraud Policy or Code of Conduct that all contacts with the media must be by an authorised individual (such as the Public relations director) and that anyone breaching the policy will be subject to disciplinary action. Media leaks can have a negative impact on the Bank's reputation.

When cases of suspected fraud are raised to the attention of senior management, the public relations department should prepare a brief for the press that can quickly be released in the event that news of the fraud does become public.

Some organisations actually choose to go public and release details of a fraud that has been uncovered. There can be advantages in being open about fraud and a publicised successful fraud investigation can give the message that the organisation takes fraud seriously and be a sharp reminder to those who may be tempted to defraud. (Samociuk et al. 2010, 129-147).

5.2.6 Measuring Fraud Resistance

Fraud resistance refers to the measure of how prepared the Bank is to withstand and cope with the threat of fraud. Fraud resistance consists of:

1. Proactive or preventative elements of the strategy which affect whether or not frauds will succeed. Tone at the top, risk assessment, risk treatment, implementation of controls, training and awareness programmes and risk follow ups are all internal elements that should be included in the Bank's preventative measures against fraud.

2. Monitoring elements which affect how quickly frauds are detected and reported. Internal audit process, monitoring the executive board, monitoring and detection and managing of incidents are the elements that are included in the monitoring measures against fraud.

3. Reactive elements are those that affect how quickly the Bank bounces back from fraud (its resilience). Managing of incidents, learning from events, review and

closure and the tone at the top comprise the third and last elements of reactive measures against fraud.

The assessment is a measure, or snapshot, of how well the Bank copes with and prevents fraud. When this assessment is performed against a baseline standard, it should be possible to identify and prioritise the improvements which need to be made. (Samociuk et al. 2010, 149-159).

RECOMMENDATIONS

Fraud prevention and detection

Ethics and training

While there is little that the Board and Bank managers can do to control the minds of employees, customers and suppliers, there are several safety precautions that they can take in order to control their actions in a bid to prevent and reduce fraud.

First, the need for management and executives to behave in an ethical manner cannot be overemphasized. If management is openly dishonest and deceitful, this example may easily work its way through the ranks. It is the responsibility of managers and executives in the Bank to uphold the Code of conduct and be on the fore-front in the fight against fraud.

The second most important measure that the Bank should take is to provide proper training to employees so that they can learn their job duties. If employees are not adequately trained, they may fail to perform their duties properly. Employees who are unable to perform well in their jobs may become tempted to commit fraud in order to get more money or receive bonuses.

Effective training programs also include training about fraud and ethical policies of the Bank. Employees must be educated about the ethical behaviour expected of them if they are going to act ethically. These ethical policies are included in the Code of Business

Conduct of the Bank and have to be upheld at all times. When ethical violations are discovered, the offenders should be punished appropriately, either by a verbal reprimand, termination or legal action. The punishment should be handed down according to the proportion of the act committed.

Third parties of the Bank, such as customers, suppliers and business partners also need to be given information regarding the ethical requirements of the Bank and their obligations to the Bank explained.

On several occasions also, fraudsters have taken advantage of honest and hardworking employees by deceiving them into signing documents or to override controls in order to commit fraud. According to Comer (2003, 4), "Often the best and most hard-working employees are the easiest to deceive in order to commit fraud. This is because they are so focused on their primary work that they do not necessarily pay attention to details that appear unimportant until it is too late." This statement brings to light the importance of training employees to be alert by looking out for suspicious activity and or documents and to ensure that they follow controls strictly.

The best control to reduce the likelihood of fraud committed through forged signatures on documents is to make it difficult for someone to insert a false document. The internal risk of an employee submitting false documents can be reduced by reconciling the documents coming in and going out of a department. In case a query arises, they should immediately report to their line manager or the appropriate person. The external risk can be reduced by telephoning customers or originators to verify that they dispatched the documents. Where call backs to every customer is considered to inflict much strain on available resources, Bank managers can set a limit above which a call back will be made.

Upgrading safety controls and systems

Physical security of the company premises and assets directly prevents theft and abuse of physical assets, as well as indirectly protecting the company in other ways. Good security measures should include having security guards on company premises, locked

doors and restricted access to company premises, computers, data and assets. (Coenen 2008, 50).

Most large financial institutions have implemented operational risk frameworks, which may be run using custom built or an off-the-shelf software package. Operational risks are entered into a 'risk register' which usually contains details such as the nature of the risk, the likelihood and consequences of the risk, current and suggested controls and the owner of the risk for follow-up action. The software is then used to monitor and report on management treatment of each risk. Setting up a risk register is reasonably straightforward and does not necessarily require specialist software. A standard spreadsheet or database software can be used. (Samociuk et al. 2010, 80-81).

Relationships may develop between employees and customers or suppliers of the Bank due to the fact that they have worked together for many years. Such kinds of personal relationships can facilitate fraud. Experts suggest that job rotation can cut down on the possibility of fraud by disrupting these personal connections and or even expose fraud that could be on-going. (Coenen 2008, 49).

Lost, stolen and counterfeit payment cards

Barclays Bank of Kenya handles hundreds of fraud cases annually which involve counterfeit, lost or stolen cards. According to Barclays Bank, only 30% of its customers actually possess payment cards. Worse still is that a majority of these customers do not understand fully how these cards work and how to use them safely when carrying out transactions.

Barclays Bank definitely needs to educate their customers about payment cards, how they work and safety measures. For instance, the Bank needs to emphasize to their customers to always ensure that their payment cards are in their possession at all times and that their PIN numbers are safeguarded at all times. In case one loses a payment card, the Bank should be informed as soon as possible so that the card can be cancelled immediately.

The Bank could also introduce a security measure that if one chooses to pay using his/her payment card, he/she should always produce an identification card for verifica-

tion. This measure could significantly reduce the amounts of purchases and other transactions made using stolen or lost payment cards.

The Bank issues its customers with magnetic stripe cards because it has not installed the chip card technology. A majority of fraudsters have mastered the skills and have the technology needed to produce counterfeit magnetic stripe cards because their security features are relatively easy to tamper with. The chip in chip cards offers a tamper-resistant feature and is quite expensive to produce. The chip also improves the process of determining counterfeit cards, through implementing the card authentication method with dynamic authentication mechanisms. It also provides greater protection of the cardholder against fraudulent transactions through verification of the PIN in the card, for transactions authorized off-line.

A way for the Bank to reduce frauds committed through the use of counterfeit cards would be to install the chip card technology. By implementing the chip technology, the Bank would not only reduce the amount of fraud considerably, but also would increase its competitive strategy in the long run.

Implementing the chip technology system, however, comes with an overwhelming installation and maintenance cost, and also causes disruption of normal business transactions. The host computers of the issuer (the Bank) and acquirers (its business partners such as supermarkets, hotels, and so on) as well as the payment network must be adapted for the chip technology. This means that the Bank's business partners also have to be willing to adapt the new technology and implement the necessary equipment despite the hefty costs. (Radu 2002, 55).

Reducing Travel and Entertainment fraud

Travel expenses are a normal part of many businesses because managers and or employees have to travel to different areas to carry out business duties. They therefore are very difficult to eliminate. A way of reducing fraud committed by submitting multiple travel expenses is by installing Travel & Entertainment (T&E) software for example, Concur, which generates, verifies and processes the expense claims, therefore eliminating chances of dishonesty. The Concur software allocates each T&E claim a unique set

of numbers which makes the T&E claim unique and helps to differentiate it from other T&E claims.

The T&E claims presented for compensation should be subjected to audits in order to determine their validity. While it is impossible to go through each T&E, it is worthwhile to pay more attention to those ones containing large amounts of money. Both internal and external auditors should select T&E claims randomly and subject them to the auditing process.

T&E fraud is mainly committed by managers and usually starts out small and grows with time. To prevent such growth, catching or discouraging individuals from committing travel fraud may act as a fraud deterrent. (Vona 2008, 137).

Bribery and misuse of company assets

Preventing fraud committed through bribery can be very difficult because detecting the fraud itself is not easy. However, the Bank needs to uphold its corporate policy that specifically addresses the problems and illegalities associated with bribery and related offenses. The policy makes the position of the company on bribery absolutely clear.

In a bid to reduce fraud through bribery, the Bank should strictly prohibit receiving of gifts and other favours from prospective customers and or suppliers. In case an employee receives an unsolicited gift, he/she should report it immediately to his/her supervisor and either return it or donate it to a Non-profit organization. (Rollins & Lanza, 2004, 105).

Misusing the Bank's assets, for example, making personal telephone calls or using computers for personal use is a risk that can be retained by the Bank since it does not usually cost the Bank so much money. However, this does not mean that the Bank should tolerate such behaviour. Employees and managers should be warned that if they are caught misusing company assets, action will be taken against them.

Insuring against potential fraud

Many organisations reduce fraud risks by transferring the risk to insurers through employee fidelity or computer crime policies. This can be a prudent step but an organization should carefully check the policy to ensure that losses will be covered and to be clear about the requirements for making a claim. Bank managers should discuss with insurance companies about the insurable fraud risks and where possible, take out insurance for them.

Valuable information is lost to fraudsters who steal confidential company information; worst still is that it is very difficult to estimate the monetary value of this information. However, the Bank can transfer such a risk to an insurance company. Even though the Bank might not recover all the stolen information, it will be compensated for the loss by the insurance company.

Internal and external audits

Audits are aimed at determining whether the financial statements are fairly presented and if they give an accurate account of the financial status of an organization. Auditors can only test a small fraction of transactions and direct management to correct any material errors that are found during the testing. This does not mean that auditing is not important. A study by the Association of Certified Fraud Examiners in 2006 in the US revealed that approximately 32% of fraud was discovered by both internal and external auditors. (Coenen 2008, 15). These statistics emphasize the importance of carrying out regular audits in the Bank as a means of fraud prevention and detection.
Periodic job rotations and mandatory vacations could help expose ongoing fraud in the Bank. When an employee is on leave, it is difficult for them to continuously monitor a fraud scheme. Job rotations are also effective at disrupting these schemes, especially when the employees are not given advance notice. (Coenen 2008, 39).

Fraud resolution

When it comes to reacting to fraud, there are several recommended approaches that the Bank can use. These approaches include dismissals, civil procedures and criminal prosecutions. It is important to remember that fraud cases take time to investigate and resolve, sometimes even decades. Prosecuting fraudsters sends a powerful deterrent

message across the Bank. However, there are times that a Board may decide that pursuing of a lengthy investigation or a criminal penalty may not be the most appropriate course of action.

Senior management should carefully consider the full ramifications of the approaches they choose to take, and their potential impacts on the anti-fraud culture. Also, the Board should be made aware of any potential effects on future insurance cover under fidelity or crime policies. Whatever course of action is decided upon, management should always look at what went wrong and allowed the fraud to happen. Sometimes fraud can be a symptom that the whole system is not working and it may be better to fix the whole system rather than just one problem, so avoiding large costs in the future.

In some countries or states it is a legal requirement to report fraud cases to the national police. It is beneficial to discuss a case with the police as soon as practicable, even if no complaint is subsequently filed. The police may already be investigating similar frauds which have occurred in other organisations, particularly where these involve organised criminal groups.

According the Association of Certified Fraud Examiners (ACFE) many companies do not refer their fraud cases to law enforcement. The most common reason is the fear of bad publicity, which accounted for 43% of cases. 33% of cases were not pursued because management believed that internal discipline was sufficient. 30% were not pursued because a private settlement was reached, and 21% were deemed too costly to pursue.

Many companies would rather move forward and put the fraud in the past, particularly if the fraud case involved highly visible employees. Taking action against those who commit occupational fraud prolongs the pain and is an ongoing reminder of the fraud. That prospect is not appealing to many corporate managers and likely accounts for the reason why many of the companies that don’t pursue employees who have stolen from them. (Coenen 2008, 18-19).

CONCLUSION

Fraud can be defined as intentionally deceiving or overriding controls in order to gain personal benefit while inflicting damage to the other party. Personal benefit could be in form of money, information or other assets.

No single organization is immune to fraud; fraud accounts for 5-7% of all losses incurred by organizations annually. This thesis was undertaken to find out the causes of fraud, methods used to commit fraud, fraud detection and actions taken against fraudsters in Barclays Bank of Kenya. By so doing, the writer would create a more understanding of fraud among employees and third parties of the Bank and present her findings which would be used to mitigate the probability of fraud occurring and reduce its consequences drastically.

In order for this thesis to materialize, the writer had to make use of several sources to find information regarding the topic. A questionnaire was sent to a fraud specialist at the Bank who provided information regarding the Bank, fraud statistics in the Bank, existing controls and resolution guidelines followed by the Bank upon detection of fraud. Other sources of information include references from books in the area of fraud, local newspapers, websites and journals.

Reducing fraudulent activities in the Bank is one way of ensuring that quality standards of the Bank are improved. Improving quality within Barclays Bank of Kenya could be done through collecting information from customers regarding the Bank and its services and using this information to streamline its business processes.

The Bank as a whole, should strive to ensure that customer needs and requirements and met sufficiently and economically. For this to be possible, processes carried out within the bank and the employees who carry out these processes, should each play a vital role in ensuring that quality is valued and upheld at all times.
Employees, despite how innocent they may look, suppliers, customers and even business partners are all capable of committing fraud. Other culprits include criminal groups, governments and competitors. Armed with this information, it pays to be always vigilant of suspicious activities and train employees and third parties to be alert to fraud. The Bank’s code of conduct should be communicated to employees and third parties alike and the actions taken against fraudsters made clear to everyone. The management

and executives of the Bank need to uphold strong ethical character which should be resonated throughout the Bank.

The major types of fraud identified by the Bank include: identity theft and use of lost or stolen documents, use of counterfeit cards, bribery and conflicts of interest, misuse of company assets, theft of confidential information, cheque fraud and fund transfers, Travel and Entertainment fraud and money laundering.

In order for Barclays Bank of Kenya to be able to prevent and reduce these frauds to the minimum, the fraud risk assessment team of the Bank should follow the six-step fraud risk assessment strategy which provides guidelines that help to prevent, detect, manage and resolve fraud.

The first step in the assessment of fraud is to develop an anti-fraud culture in the Bank which is only attainable with the full support of the Board and top management. The Board of Directors and top management need to set an example to their subordinates by behaving in an ethical manner according to the Bank's Code of Conduct. There is a need to ensure that all employees of the Bank fully understand fraud, risks posed by fraud and their repercussions to the Bank. A strong anti-fraud stand should be upheld by the management and Board and should be emphasized throughout the organization.
The next step is to assess fraud risks through collecting as much information as possible regarding fraud in the Bank. The information is collected through interviewing employees and managers, from past financial documents, analyzing information and transactions in computer systems, reviewing control systems and reviewing information regarding third-parties.

The third step is to treat fraud risks that were detected during assessment. Treating fraud is based on the likelihood of a certain type of fraud occurring and the impact it has on the Bank. Fraud treatment measures include avoiding fraud risks, transferring fraud risks, retaining the risks and or reducing the likelihood or consequences of fraud. Whichever measure is decided upon depends on the severity of the fraud and needs to be carefully thought-out.

There are several ways that fraud can be detected. These include whistle blowers, who are people that report suspicious activities, accidentally, though audits, and or through pre-emptive health checks. Through detection, many frauds are prevented from actually occurring. Employees and managers alike need to be trained to become more alert in their jobs and activities. Once a red flag has been detected, employees need to report it immediately to their supervisors. Whistle blowers should be protected in order to safe-guard their identity and jobs. Once red flags have been reported, they need to be discreetly followed upon in order to determine their validity.

The fifth step is to manage incidents related to fraud. After a possible fraud has been detected, the risk assessment team needs to carefully follow up the issue with as minimum disruption to normal business activities as possible. The team needs to be discreet in order to ensure that the culprits are not alerted and thereby destroy evidence.

Incase the fraud scandal leaks to the media or public, the Public Relations department of the Bank should contain the situation as soon as possible and issue a statement on the scandal but however, avoid disclosing information that is still under investigation.

Another measure that the Bank needs to take is to dismiss the dishonest employees and hire an investigator to follow up on the issue, in case its assessment team does not have the capability. The Bank should also inform the local police about the culprits in question. The Bank should file a case against the fraudsters in a court of law in order to communicate its anti-fraud stand. Sometimes however, prosecuting fraudsters may not be the best cause of action as cases can take years to investigate and could cost the Bank more than the actual fraud. Whatever the cause of action taken against fraudsters depends entirely on the Bank and the severity of the fraud.

The last step is to measure fraud resistance in the bank. This is done by examining how effectively the improved controls are working, employees' knowledge level of fraud and fraud prevention and the general attitude towards fraud in the Bank. Measuring fraud resistance shows how prepared the Bank is to fraud and how it copes with fraud.

Through preventing and reducing fraud, the Bank will prevent the loss of millions of Kenya shillings to fraudsters and will increase confidence among its customers and other stakeholders. By so doing, the quality of output, such as services and corporate responsibility programs provided by the Bank will improve considerably. Improving the

quality of the Bank's transactions directly improves its image in the market and sets the Bank apart from its competitors.

The fight against fraud seems to be an uphill battle which leaves many wondering if it can be achieved. Despite having rules and regulations that govern our actions and limit out rights, some people still find ways of defying these systems and set their own rules of the game. These are the very people who, in the concept of fraud, are referred to as fraudsters. Unfortunately, there is no way of controlling another person's mind or actions.

With the advancement of technology, the availability of abundant information and increased globalization, humans will continue to face the challenge of identity theft and fraud. Technology not only enhances positive innovation and communication but also, harbours a wave of potential information loss through hacking. Being avid users of the internet puts us at direct risk of losing our valuable information to potential fraudsters.

REFERENCES

Adam, Jolly. 2005. Managing Business Risk. 2nd Edition. GBR: Kogan Page Ltd.

Angira, Zadock. 2011. Theft of cash from ATMs on the rise. Printed 25.11.2011. http://www.nation.co.ke

Arthur, Diane. 2005. Recruiting, Interviewing, Selecting and Orienting New Employees. 4th Edition. USA: Saranac Lake, NY, AMACOM Books.

Barclays Bank PLC. 2011. http://www.barclays.com/africa/kenya/index.php

Bhat, K. Shridhara. 2010. Total Quality Management. IND: Mumbai, Global Media.

Biegelman, Martin T. 2009. Identity Theft Handbook: Detection, Prevention and Security. USA: Hoboken, NJ, Wiley.

Coenen, Tracy. 2008. Essentials of Corporate Fraud. USA: Hoboken, NJ, Wiley.

Comer, Michael J & Maxima Group Plc Staff (Contributor). 2003. Investigating Corporate Fraud. GBR: Abingdon, Oxon, Gower Publishing Limited.

Goldmann, Peter D & Kaufman, Hilton. 2009. Anti-Fraud Risk and Control. USA: Hoboken, NJ, Wiley.

Grosse, Robert E. 2001. Drugs and Money: Laundering Latin America's Cocaine Dollars. USA: Westport, CT, Greenwood Press.

Hampton, John J. 2009. Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity. USA: Saranac Lake, NY, AMACOM Books.

Hi. World Trade Center. 1998-2011. http://www.hiwtc.com/products/magnetic-stripe-card-membership-card-2054-8144.htm

Jeyarathmm, M. 2008. Strategic Management. IND: Mumbai, Global Media.
Lal, H. 2008. Organizational Excellence Through Total Quality Management. IND: New Age International.

K.H. Spencer Picket. 2007. Corporate Fraud: A Manager's Journey. USA: John Wiley & Sons, Inc.

MasterCard. 1994-2011.
http://www.mastercard.com/au/personal/en/education/chipcard.html

Radu, Cristian. 2002. Implementing Electronic Card Payment Systems. USA: Norwood, MA, Artech House.

Rollins, Steven C & Lanza, Richard. 2004. Essential Project Investment Governance and Reporting: Preventing Project Fraud and Ensuring Sarbanes-Oxley Compliance. USA: J. Ross Publishing, Incorporated.

Samociuk, Martin, Iyer, Nigel & Doody, Helenne. 2010. Short Guide Fraud Risk: Fraud Corruption Resistance and Detection. 2nd Edition. GBR: Farnham, Surrey, Ashgate Publishing Group.

Tian, Kelly Tepper & Keep, Bill. 2001. Customer Fraud and Business Responses: Let the Marketer Beware. USA: Westport, CT, Greenwood Press.

USLegal, Inc. 2001-2011.http://definitions.uslegal.com/b/bank-fraud/

APPENDIX

Research Questions

1. What are the reporting guidelines of fraud in the Bank?

2. Why do you think that fraudulent activities occur within and against the Bank?

3. What are the different types of fraud that witnessed by the Barclays Bank of Kenya?

4. What are some of the impacts of fraud on the Bank?

5. On average, how many cases of fraud are witnessed annually by Barclays Bank of Kenya?

6. What is the average amount of money (in Kenya Shillings) that the Bank loses to fraud yearly?

7. What are the general methods of fraud detection used by the Bank?

8. Once fraud is detected, what are the actions taken by the Bank against the fraudsters?

9. What percentages of fraudsters who are caught by the Bank are actually prosecuted yearly?